UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /aba	8250

7380 7590 11/13/2008

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	**PAPER NUMBER**
3685	
MAIL DATE	**DELIVERY MODE**
11/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/702,540	**Applicant(s)** SO, VINCENT
	Examiner CHARLES C. AGWUMEZIE	**Art Unit** 3685

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-23,34-36 and 38-54* is/are pending in the application.

4a) Of the above claim(s) *1, 4-15, 35-36, and 38-53* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-23, 34 and 54* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11/7/03; 9/28/07*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election with traverse of claims 16-23, 34 and 54 in the reply filed on August 1, 2008 is acknowledged. In view of Applicant's amendments the restriction requirements with respect to claim 34 is withdrawn because independent claim 34 recites common feature that decryption key is only destroyed after the next decryption key is received. Accordingly claims 16-23, 34 and 54 have been examined.

Response to Arguments

2. Applicant's arguments filed April 7, 2008 have been fully considered but they are not persuasive.

3. With respect to **claims 16 and 34**, Applicant argues that there is no suggestion whatsoever in Feig et al. that each decryption key is delivered and then deleted or destroyed after decryption of the corresponding encrypted content segment in a manner that would prevent the client from simultaneously having possession of all of the decryption keys. In fact, Feig et al. clearly states that token keys (decryption keys) are retained by the customers once they are delivered.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Applicant responds to the rejection by attacking the references separately, even though the rejection is based on the combined teachings of the references. Nonobviousness cannot be established by attacking the references individually when the rejection is predicated upon a combination of prior art disclosures.

4. Applicant further argues that Giroux et al invention prevents the customer from simultaneously having possession of more than a single decryption key because the next decryption key for the next encrypted segment is not delivered to the customer until customer requests the next decryption key after the decryption of current encrypted segment is completed, the decrypted information is displayed and the current decryption key has been deleted.

In response, Examiner reminds Applicant that it has been held that broadly providing an automatic or mechanical means to replace a manual activity which accomplished the same result is not sufficient to distinguish over the prior art.) *In re Venner*, 262 F.2d 91, 95, 120 USPQ 193, 194 (CCPA 1958). Besides, Gioux's customer processing platform has at most a subset of the decryption keys corresponding to the encrypted sections of data content when customer has possession of the decryption keys for the current section of the encrypted information. The next key is present because when the customer moves to a different section of the encrypted content, the previous content and decryption key is deleted and the process is repeated.

5. With respect to **claims 17-18**, Applicant argues that dependent claims 17-18 are patentable by virtue of its dependency from claim 16.

In response, Examiner respectfully disagrees and submits that claims 17-18 are not patentable being dependent from claim 16.

6. With respect to **claim 19**, Applicant argues that dependent claim 19 is patentable by virtue of its dependency from claim 16.

In response, Examiner respectfully disagrees and submits that claim 19 is not patentable being dependent from claim 16.

7. With respect to **claim 20**, Applicant's argument is moot in view of new grounds of rejection.

8. With respect to **claims 22-23**, Applicant argues that dependent claims 22-23 are patentable by virtue of its dependency from claim 16.

In response, Examiner respectfully disagrees and submits that claims 22-23 are not patentable being dependent from claim 16.

9. With respect to **claims 1, 4, 5, 6-15, 35-36, 38-53**, Applicant's argument is moot by virtue of their withdrawal from further consideration pursuant to a restriction requirements.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 16-18**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1.

12. As per **claims 16 and 21**, Feig et al discloses a method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key (fig. 3; steps 302-314; col. 1, line 55-col. 2, line 10, which discloses "plurality of sequential data blocks using corresponding token key");

and for each encrypted section:

receiving a decryption key in respect of the encrypted section (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys…and for playing back each recovered sequential data");

decrypting and playing back the encrypted section using the decryption key (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys…and for playing back each recovered sequential data");

destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content.

13. What Feig et al does not explicitly teach is

destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content.

14. Giroux et al discloses a method comprising:

destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...when the user moves to a different section the process is repeated…." See claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received, such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content in view of the teachings of Giroux et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

15. As per **claim 17**, Feig et al failed to explicitly disclose the method, further comprising, for each encrypted section:

destroying decrypted data content at the customer processing platform after completing playback of the encrypted section.

Giroux et al discloses a method comprising destroying decrypted data content at the customer processing platform after completing playback of the encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Giroux et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

16. As per **claim 18**, Feig et al discloses the method, wherein the communications medium is the public Internet (col. 1, lines 40-50).

17. As per **claim 54**, Feig et al failed to explicitly disclose the method, wherein destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section.

Giroux et al discloses the method, wherein destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key..."; see claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method wherein destroying the decryption key only after at least a decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section in view of the teachings of Giroux et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

18. **<u>Claim 19</u>**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Granger et al U.S. Patent No. 6,334,189 B1.

19. As per **<u>claim 19</u>**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein, for each encrypted section, the encryption key is the same as the decryption key.

Granger et al discloses the method, wherein, for each encrypted section, the encryption key is the same as the decryption key (col. 10, lines 45-55, which discloses that …"the decryption key is the same as the encryption key…").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method wherein, for each encrypted section, the encryption key is the same as the decryption key in view of the teachings of Granger et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

20. **Claims 22-23**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Watanabe U.S. Patent No. 7,114,073 B2

21. As per **claim 22**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

Watanabe discloses the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform (col. 5, lines 17-35, which discloses that “the encryption key generating unit 105 generates the encryption key on the basis of an IP address of a user to whom the digital content is to be transmitted”).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant’s invention to modify the method of Feig et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Watanabe in order to ensure that content is only used by authorized users.

22. As per **claim 23**, Feig et al further discloses the method, wherein receiving each decryption key comprises receiving a transmission value that is determined based on the decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the decryption key from the transmission value (col. 2, lines 40-65).

23. **Claim 20,** is are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 as applied to claim 16 above, and further in view of Schull U.S. Patent Application Publication No. 2007/0219918 A1.

24. As per **claim 20**, Feig et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

Schull discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform (see fig. 1; 0031; 0037; 0038; 0084; note that cryptographic keys are generated in pair with the encryption key corresponding to the decryption key).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of feig et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Schull in order to encourage wider distribution of content to other participants.

25. Claims **34**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Feig et al U.S. patent No. 7,251,833 B2 and further in view of Giroux et al U.S. Patent No. 2002/0078361 A1.

26. As per **claim 34**, Peterka et al further discloses a method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device (0072; 0123; 0145);

comparing the customer verification information with corresponding stored customer information (0145); and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer (figs. 8 and 9);

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted data content (fig. 5; 0145); and

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data.

27. What Peterka et al does not explicitly teach is

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data.

causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted data.

28. Feig et al discloses:

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data (col. 2, lines 40-65, “one to one decryption”).

29. Giroux et al discloses a method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device such that at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted data (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key..."; see claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant’s invention to modify the method of Peterka et al and incorporate the method of causing a key for a preceding portion of the encrypted data to be deleted from the customer data content processing device in view of the teachings of Giroux et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Conclusion

30. **Examiner’s Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art ad are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Calvin Hewitt** can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685

November 7, 2008